

Blockchain and Cryptocurrency

Venkatesan Subramanian

1 Component - 2

- The students of old ordinance need to study the Bitcoin and Ethereum from the draft book by Venkatesan Subramanian, Sandeep Kumar Shukla and Mohan Dawan. The basic slides and book draft are already shared with you all.
- The students of new ordinance (CCLCAA) need to study Ethereum. The basic slides and book draft by Venkatesan Subramanian, Sandeep Kumar Shukla and Mohan Dawan are already shared with you all.

1.1 Assignment for New Ordinance

1.1.1 Theory

- In ethereum public network, as of now how many addresses are there and what is the size of merkle patricia tree. If required download the main network block from any source and check the size.
- Like ethereum, find the number of addresses used till now in Bitcoin.
- As present time, a node with 2GB GPU can act as a miner of Ethereum main network or not.
- Analyze and differentiate the Patricia tree and Radix tree
- How the size of DAG in ethereum ETHASH grows when the height of the DAG remains same?

1.1.2 Lab

- Write the structure of Merkle patricia tree in *C* language.
- Implement the hash pointer using the *Go* language.
- Write an Ethereum smart contract for simple Election voting and find the number of gas needed. This can be tested in Truffle or other test networks.

1.2 Assignment for Old Ordinance

Study the paper Algorand [209] and complete the table 1.2.

Parameter	Bitcoin	Ethereum	Algorand
Cryptocurrency	Yes	Yes	
DAPP	No	Yes	
How it works	Trans.	Balance	
Consensus	PoW	PoW	
Above algorithm	Prob.	Prob.	
Confirmation Time	Avg 10 m	Avg 15 s	
Fork	Yes	Yes	
Waiting time	7 Blocks	23 Blocks	
Decentralization	Yes	Yes	
Authority	No	No	
Permissionless	Yes	Yes	
World State	No	Yes	

References

- [1] Algorand - <https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf>, [Last Accessed on 17/03/2020].